PSEUDO-ELLIPTIC INTEGRALS, UNITS, AND TORSION

FRANCESCO PAPPALARDI AND ALFRED J. VAN DER POORTEN

ABSTRACT. We remark on pseudo-elliptic integrals and on exceptional function fields, namely function fields defined over an infinite base field but nonetheless containing non-trivial units. Our emphasis is on some elementary criteria that must be satisfied by a squarefree polynomial whose square root generates a quadratic function field with non-trivial unit. We detail the genus 1 case.

1. Pseudo-Elliptic Integrals

The surprising integral

$$\int \frac{6x\,dx}{\sqrt{x^4+4x^3-6x^2+4x+1}} = \log\Big(x^6+12x^5+45x^4+44x^3-33x^2+43 \\ +(x^4+10x^3+30x^2+22x-11)\sqrt{x^4+4x^3-6x^2+4x+1}\,\Big)$$

is a nice example of a class of pseudo-elliptic integrals

$$\int \frac{f(x)dx}{\sqrt{D(x)}} = \log\big(a(x)+b(x)\sqrt{D(x)}\big). \tag{1}$$

Here we take D to be a monic polynomial defined over $\mathbb{Q}$, of even degree $2g+2$, and not the square of a polynomial; f, a, and b denote appropriate polynomials. We suppose a to be nonzero, say of degree m at least $g+1$. We will see that necessarily $\deg b = m-g-1$, that $\deg f = g$, and that f has leading coefficient m. In our example, $m=6$ and $g=1$.

Plainly, if (1) holds then it remains true with $\sqrt{D}$ replaced by its conjugate $-\sqrt{D}$. Adding the two conjugate identities we see that

$$\int 0\,dx = \log\big(a^2-Db^2\big). \tag{2}$$

Thus a^2-Db^2 is some constant k, and must be nonzero because D is not a square. In other words, $u=a+b\sqrt{D}$ is a nontrivial unit in the function field $\mathbb{Q}(x,\sqrt{D})$; and $\deg a = m$ implies $\deg b = m-g-1$ is immediate.

Differentiating (2) yields $2aa'-2bb'D-b^2D'=0$. Hence $b\big|aa'$, and since a and b must be relatively prime because u is a unit, it follows that $b\big|a'$. Set $f=a'/b$,

Typeset February 1, 2008 [16:37].
2000 *Mathematics Subject Classification.* Primary 11G30, 14H05; Secondary 33E05.
Key words and phrases. quadratic function field of characteristic zero.
This paper was constructed during a visit by the second author to Italy supported in part by a GNSAGA INDAM grant; his work is also supported by a grant from the Australian Research Council.

noting that indeed $\deg f = g$ and that f has leading coefficient m because a and b must have the same leading coefficient.*

Moreover,

$$u' = a' + b'\sqrt{D} + bD'/2\sqrt{D} = a' + (2bb'D + b^2D')/2b\sqrt{D} = a' + aa'/b\sqrt{D}\,.$$

So, remarkably, $u' = f(b\sqrt{D} + a)/\sqrt{D} = fu/\sqrt{D}$.

Thus, to verify (1) it suffices to make the not altogether obvious substitution $u(x) = a + b\sqrt{D}$, of course given that u is a unit of the order $\mathbb{Q}[x, \sqrt{D}\,]$.

Remark. The case $g = 0$, say $D(x) = x^2 + 2vx + w$, is useful for orienting oneself. Here $(x + v) + \sqrt{D}$ is a unit, of norm $v^2 - w$, and indeed

$$\int \frac{dx}{\sqrt{x^2 + 2vx + w}} = \operatorname{arsinh} \frac{x + v}{\sqrt{w - v^2}} = \log\bigl(x + v + \sqrt{x^2 + 2vx + w}\,\bigr)\,.$$

Notice that $\deg f = 0$ and has leading coefficient 1, as predicted.

2. Units in Quadratic Extension Fields, and Torsion

2.1. **Number fields.** Let N be a positive integer, not a square, and set $\omega = \sqrt{N}$. It is easy to apply the Dirichlet box principle to prove that an order $\mathbb{Z}[\omega]$ of a quadratic number field $\mathbb{Q}(\omega)$ contains nontrivial units. Indeed, by that principle there are infinitely many pairs of integers (p, q) so that $|q\omega - p| < 1/q$, whence $|p^2 - Nq^2| < 2\sqrt{N} + 1$. It follows, again by the box principle, that there is an integer l with $0 < |l| < 2\sqrt{N} + 1$ so that the equation $p^2 - Nq^2 = l$ has infinitely many pairs (p, q) and (p', q') of solutions with $p \equiv p'$ and $q \equiv q' \pmod{l}$. For each such distinct pair, $al = pp' - Nqq'$, $bl = pq' - p'q$, yields $a^2 - Nb^2 = 1$.

2.2. **Function fields.** Just so, in the function field case already introduced, there are infinitely many pairs of polynomials $p(x)$ and $q(x)$ so that $\deg(q\sqrt{D} - p) < -\deg q$, whence $\deg(p^2 - Dq^2) \le g$. But a second application of the box principle fails when the base field, $\mathbb{Q}$ in our introductory discussion, is infinite; because there are then infinitely many distinct polynomials of bounded degree. In that case, the existence of a nontrivial unit (thus, one not an element of the base field) is unusual happenstance. Accordingly, we say that a function field $\mathbb{Q}(x, \sqrt{D})$ with a nontrivial unit $a+b\sqrt{D}$ is an *exceptional* function field and we call D an *exceptional* polynomial.

2.3. **Torsion on the Jacobian of a hyperelliptic curve.** A slight change of viewpoint, emphasising the hyperelliptic curve $\mathcal{C} : y^2 = D(x)$, may clarify matters. A function $u = a + by$ is a unit precisely if its divisor is supported only at infinity. However, $\mathcal{C}$ has two points at infinity, say O and S (or ∞_- and ∞_+ if one prefers) and so the divisor of u is some multiple, say $m(S - O)$, of the divisor $S - O$ at infinity. Because u is a function, this is to say that the class of $S - O$ on the Jacobian of $\mathcal{C}$ is torsion of order m. In the case $\deg D = 4$, so genus $g = 1$ if D is squarefree, we may take O as the zero of the elliptic curve $\mathcal{C}$ and report that the point S on $\mathcal{C}$ is torsion of order $m = \deg a$.

*That common coefficient is 1 without loss of generality since we may freely choose the constant produced by the indefinite integration.

3. Exceptional Quadratic Fields.

It is appropriate to identify straightforward properties of the squarefree polynomial $D(x) = y^2$ sufficient or just necessary that the field $\mathbb{Q}(x, y)$ be exceptional.

Suppose therefore that $\mathbb{Q}(x, y)$ is exceptional, so that we have a unit $u = a + by$ or, more helpfully, an identity $b^2D = a^2 - k$ with $a, b \in \mathbb{Q}[x]$ and $k \in \mathbb{Q} \setminus \{0\}$. It will be helpful to set $k = c^2$. We note immediately that the two polynomials $a - c$ and $a + c$, which are conjugate over $\mathbb{Q}$ if k is not a square, are relatively prime.

We have $b^2D = (a-c)(a+c)$. Hence if k is not a square, b must factor in $\mathbb{Q}(c)[x]$ as a norm $d\overline{d}$, where the overline $\overline{}$ denotes conjugation in the quadratic extension $\mathbb{Q}(c)$, and D factorises over $\mathbb{Q}(c)$ as the product of the polynomial $(a - c)/d^2$, and of its conjugate. In particular, $\deg b = m - g - 1$ must be even.

If, however, k is a square in $\mathbb{Q}$ (thus, in particular, always if $\deg b = m - g - 1$ is odd) then we seem to see only that b must have a factor d defined over $\mathbb{Q}$ so that both $2 \deg d$ and $2m - (2g + 2) - 2 \deg d$ do not exceed $m = \deg(a - c) = \deg a$. That is, we have $m - (2g + 2) \le 2 \deg d \le m$.

Theorem 1. *Set $y^2 = D(x)$, with D monic, squarefree, and of degree $2g + 2$. Suppose the domain $\mathbb{Q}[x, y]$ contains a unit of degree $m > g$ and norm k.*

(a) *If m and g have the same parity then $k = c^2$ is a square.*

(b) *If $k = c^2$ is a square, there is a positive integer s so that D is a product of polynomials over $\mathbb{Q}$ of degrees $m - 2s$ and $2g + 2 + 2s - m$. Thus D is reducible over $\mathbb{Q}$ if m is odd.*

(c) *If $k = c^2$ is not a square in $\mathbb{Q}$ then D factorises over $\mathbb{Q}(c)$ as a product of two polynomials conjugate over $\mathbb{Q}(c)$, so each of degree $g + 1$.*

Note that the compactly written assertion (b) includes the possibility that D is irreducible if m is even, and (since both the stated degrees must be nonnegative) that it implicitly entails upper and lower bounds on the integer s. Assertion (c) implies that the Galois group of D is restricted by $\#\,\mathrm{Gal}(D)\big|2\big((g+1)!\big)^2$. Thus, if $g = 1$ it is the dihedral group on four elements or one of its subgroups.

We observe also that the statements of the theorem, which refer only to the polynomial D and the torsion order m, do not include all the information that may be extracted from the remarks preceding the proclamation of the theorem.

Remarks. It should be no surprise that none of the criteria of the theorem suffice to guarantee obtaining an exceptional quadratic function field. We detail the case $g = 1$ in §6 at page 74 below.

4. Continued Fractions

4.1. **Number fields.** There is a well known algorithm in the number field case yielding the fundamental unit of the order $\mathbb{Z}[\sqrt{N}]$. As before set $\omega = \sqrt{N}$ and suppose A is the integer part of ω. The zero-th step in the continued fraction expansion of $\omega + A$ is

$$\omega + A = 2A - (\overline{\omega} + A) \tag{3}$$

and a typical consequent step is of the shape

$$(\omega + P_h)/Q_h = a_h - (\overline{\omega} + P_{h+1})/Q_h\,; \quad \text{in brief} \quad \omega_h = a_h - \overline{\rho}_h\,.$$

Thus $P_h + P_{h+1} + (\omega + \overline{\omega}) = a_h Q_h$, and because the next complete quotient ω_{h+1} is the reciprocal of the remainder $-\overline{\rho}_h$ we must also have $(\omega + P_{h+1})(\overline{\omega} + P_{h+1}) = -Q_h Q_{h+1}$. In particular, certainly Q_{h+1} divides the norm $(\omega + P_{h+1})(\overline{\omega} + P_{h+1})$.

Here the P_h and Q_h are integers, and it is readily shown they all satisfy

$$0 < 2P_h + (\omega + \overline{\omega}) < \omega - \overline{\omega}\,, \qquad 0 < Q_h < \omega - \overline{\omega} \tag{4}$$

proving, by the box principle, that the continued fraction expansion of ω is periodic. Moreover, one notices that always both

$$\omega_h > 1 \text{ while } -1 < \overline{\omega}_h < 0, \text{ and } \rho_h > 1 \text{ while } -1 < \overline{\rho}_h < 0\,. \tag{5}$$

It follows that conjugation of the continued fraction tableau, replacing

$$\omega_h = a_h - \overline{\rho}_h \quad \text{by} \quad \rho_h = a_h - \overline{\omega}_h\,,$$

again gives a continued fraction expansion — in particular, a_h which began life as the integer part of ω_h, also is the integer part of ρ_h — reversing the order of the lines of the original expansion. Because line zero (3) is symmetric it occurs in the expansion of ρ_h, and because the expansion of $\omega + A$ is periodic it follows that it is in fact pure periodic, moreover with a symmetry: if the period length is r then the word $a_1\,, a_2\,, \ldots, a_{r-1}$ must be a palindrome.

One obtains the fundamental unit $a + b\omega$ by computing the convergent

$$[\,A\,, a_1\,, a_2\,, \ldots, a_{r-1}\,] = a/b\,. \tag{6}$$

4.2. **Function fields.** Mutatis mutandis, the function field argument is identical. We set $y^2 = D(x)$ as before. Plainly we may write D as $D = A^2 + R$, where $\deg A = g + 1$ and $\deg R < g$; then A is the polynomial part of the Laurent series $y \in \mathbb{Q}((x^{-1}))$. We expand $y + A$ in complete analogy with the numerical case, but now selecting the partial quotients a_h as the polynomial part of the respective complete quotients $y_h := (y + P_h)/Q_h$. The bounds (4) become

$$\deg P_h = g + 1 \quad \text{and} \quad \deg Q_h \le g \tag{4$'$}$$

and of course do not guarantee periodicity, because the base field $\mathbb{Q}$ is infinite. The conditions (5) for reduction turn into

$$\begin{aligned} &\deg(y + P_h) > \deg Q_h \quad \text{but} \quad \deg(\overline{y} + P_h) < \deg Q_h \\ &\quad \text{and} \quad \deg(y + P_{h+1}) > \deg Q_h \quad \text{but} \quad \deg(\overline{y} + P_{h+1}) < \deg Q_h\,. \end{aligned} \tag{5$'$}$$

As in the number field case, conjugation reverses the continued fraction tableaux. Thus, *if* the expansion of $y+A$ happens to be periodic then it has the symmetries of the number field case and the continued fraction expansion yields a unit of norm 1, given by the convergent (6).

4.3. **Quasi-periodicity.** Suppose now that D is exceptional in that the function field $\mathbb{Q}(x, y)$ contains a unit u, of norm $-\kappa$. By general principles that entails that some Q_i is $\pm\kappa$, say $Q_r = \kappa$ with r odd. That is, line r of the continued fraction expansion of $y + A$ is

line r: $$y_r := (y + A)/\kappa = 2A/\kappa - (\overline{y} + A)/\kappa\,;$$

here we have used (5$'$) to deduce that necessarily $P_r = P_{r+1} = A$. We recall that

line 0: $$y + A = 2A - (\overline{y} + A)\,.$$

By conjugation of the $(r+1)$-line tableau showing that $y+A$ is quasi-periodic we see immediately also that

line $2r$: $$y_{2r} := y + A = 2A - (\overline{y} + A)\,,$$

so that in any case if $y+A$ has a quasi-periodic continued fraction expansion then it is periodic of period twice the quasi-period. This is a result of Tom Berry [3]; it applies to arbitrary quadratic irrational functions whose trace† is a polynomial. Other elements $(y+P)/Q$ of $\mathbb{Q}(x,y)$, with Q dividing the norm $(y+P)(\overline{y}+P)$, may be honest-to-goodness quasi-periodic, that is, not also periodic.

Further, if $\kappa \neq -1$ then r *must* be odd. To see that, notice the identity

$$B[\,Ca_0\,,\,Ba_1\,,\,Ca_2\,,\,Ba_3\,,\,\ldots\,] = C[\,Ba_0\,,\,Ca_1\,,\,Ba_2\,,\,Ca_3\,,\,\ldots\,],$$

reminding one how one multiplies a continued fraction expansion by some quantity; this cute formulation of the multiplication rule is due to Wolfgang Schmidt [19]. The 'twisted symmetry' occasioned by division by κ, equivalent to the existence of a non-trivial quasi-period, is noted by Christian Friesen [7].

In summary, if quasi-periodic it is periodic, and the continued fraction expansion of $y = \sqrt{D}$ has the symmetries of the more familiar number field case, as well as twisted symmetries occasioned by a nontrivial κ.

Remarks. The conclusion just stated is surely well known. Certainly it is asserted by Adams and Razar [1], but without the couple of lines of argument we add here. The second of us is indebted to notes of Ethan Street [20], and related enquiries from Brian Conrad, for being reminded of this unneeded gap in the literature and of the desirability of detailing a straightforward argument. A much clumsier version of the story told here is given in [17], however with additional introductory details that may be helpful to the reader.

Theorem 2. *Set $\mathcal{C} : y^2 = D(x)$, with D monic, squarefree, and of degree $2g+2$. Suppose the divisor at infinity on the Jacobian of the curve $\mathcal{C}$ is torsion of order $m > 1$, equivalently the domain $\mathbb{Q}[x,y]$ is exceptional in containing nontrivial units, and its fundamental unit $u = a + by$ is of degree m, and say of norm k. Denote the continued fraction expansion of y by $y = [\,A\,,\,a_1\,,\,a_2\,,\,a_3\,,\,\ldots\,]$. Then, further to Theorem 1,*

(a) *If $[\,A\,,\,a_1\,,\,a_2\,,\,\ldots\,,\,a_{r-1}\,] = a/b$ with r even, then $k=1$.*

(b) *If $k = c^2$ is a square, then the polynomial b factorises over $\mathbb{Q}$ as say $b = d_+d_-$, and D is reducible over $\mathbb{Q}$ because it factorises as the product of the nontrivial polynomials $(a+c)/d_+^2$ and $(a-c)/d_-^2$.*

(c) *If $k = c^2$ is not a square in $\mathbb{Q}$ then the polynomial b factorises over $\mathbb{Q}(c)$ as a product $b = d\overline{d}$ of polynomials conjugate over $\mathbb{Q}(c)$, and D factorises over $\mathbb{Q}(c)$ as a product of the two polynomials $(a+c)/d^2$ and $(a+\overline{c})/\overline{d}^{\,2}$.*

For $g=1$ we must have $m = r+1$ by the bounds $(4')$, so the parities of m and r are of course different; in particular, m odd entails the norm $k=1$. One readily notices that symmetry implies that always if r is odd the parities of m and g are different; the converse is not true if $g>1$. For the rest, Theorem 2 fills in details omitted from Theorem 1.

†If y has trace t, rather than zero trace, replace line zero of the expansion by $y + A - t = 2A - t - (\overline{y} + A - t)$ and so on in the story just told. To be able to do that t should of course be 'integral', that is, a polynomial.

An important such 'detail', is the observation that if, say, $2\deg d_+ = m$ so $d_+^2 = a + c$, then $Dd_-^2 = a - c = d_+^2 - 2c$. So also $d_+ + yd_-$ is a unit of $\mathbb{Q}[x, y]$ plainly contradicting the minimality of m, that is, that u is a fundamental unit.

Furthermore, we see that D has a factor of degree at most g if the period length $r = 2h$ is even. For then, by conjugation, the line

$$(y + P_h)/Q_h = a_h - (\overline{y} + P_{h+1})/Q_h$$

is symmetric, that is $P_{h+1} = P_h$, and so Q_h divides P_h. But then Q_h also divides the norm $(y + P_h)(\overline{y} + P_h)$ and that entails Q_h is a factor of D.

There are contexts in which one would like to be certain that a polynomial D is *not* exceptional. Our results have the following consequence.

Corollary 3. *If a monic polynomial D of even degree is irreducible and with Galois group the full symmetric group then D is not exceptional; that is, the continued fraction expansion of $\sqrt{D}$ is* not *periodic.*

5. Exceptional Polynomials

In practice, the start of the continued fraction expansion of $y = \sqrt{D}$ quickly reveals whether or not D is exceptional. For example, it is shown in [1] for $g = 1$ that in $y_h = (y + P_h)/Q_h$ the divisor of Q_h is $h + 1$ times the divisor at infinity. Thus, by well known properties of Neron–Tate height, the number of decimal digits of the numerators and denominators of the coefficients of Q_h (and then also of P_h) is $O(h^2)$ unless the divisor at infinity is torsion. Moreover, in practice that explosion in complexity of the Q_h is immediately evident; see [15] for an example. Moreover, that same explosion in complexity occurs for arbitrary $g > 0$ since it follows from addition on the Jacobian of the curve $y^2 = D(x)$ being given by composition of quadratic forms, that is, by the continued fraction expansion of y; [5] or [11] explain this connection. In any case, [4], the matter of explosion of complexity of Padé approximants of algebraic functions of positive genus is far more general yet.

In the number field case, the fundamental unit of an order $\mathbb{Z}[f\omega]$ is some power of the fundamental unit of the domain of all integers of $\mathbb{Q}(\omega)$. For function fields over a base field of characteristic zero, however, an order $\mathbb{Q}[x, f(x)y]$ need not possess a unit at all, notwithstanding that $D = y^2$ be exceptional. In other words, periodicity of y does not at all guarantee quasi-periodicity of fy for a polynomial f of positive degree. The requirement in our theorems that D be squarefree thus really does matter. Specifically, although the continued fraction expansion is trivially quasi-periodic for $\deg D = 2$, thus $y^2 = D$ of genus $g = 0$, this may not hold for $y^2 = f^2D$, even though that curve is of genus 0. There are interesting papers, see [9] and its references, discussing this issue.

6. The Quartic Case

The case $g = 1$ is completely known over $\mathbb{Q}$, see [16] and its references, or for example [2]. In particular, one knows by Mazur's Theorem [13] that the only possibilities for m are $m = 2, 3, \ldots, 10$, and 12. From [18] one learns that in the cases $m = 10$ and $m = 12$ it happens that in fact $k = c^2$ never is the square of a rational.

For torsion $m \geq 4$ one may take D_m as $(X^2 + v - w^2)^2 + 4v(X + w)$ without loss of generality; $D_3(X) = (X^2 - w^2)^2 + 4v(X + w)$, while $D_2(X) = (X^2 + u)^2 + 4w$.

Theorem 4. *Set $\mathcal{C}_m : y^2 = D_m(x)$, with D_m monic, squarefree, and of degree 4. Suppose the divisor at infinity on the Jacobian of the curve $\mathcal{C}_m$ is torsion of exact order $m > 3$. Then $D_m(x;t)$ is reducible over $\mathbb{Q}$ if m is odd or in the cases listed in Table II. Otherwise, its Galois group is the dihedral group $\mathcal{D}_4$, other than for the exceptions listed in Table I.*

Proof. We know from above that $D_m(x,t)$ is reducible if m is odd or if the norm $k_m(t)$ of the fundamental unit happens anyhow to be a square. Specifically, [18] reports that $k_8(t) = 4(t-1)(2t-1)^2/t^3$, $k_6(t) = 4t$, and $k_4(t) = 4t$, explaining several of the entries in Table II. Thus we may suppose that $k = c^2$ with c quadratic irrational over $\mathbb{Q}$.

The Galois group G_D of $D = D_m$ is the dihedral group $\mathcal{D}_4$ exactly when the zeros of D are α_1, α_3, $\alpha_2 = \overline{\alpha}_3$, and $\alpha_4 = \overline{\alpha}_1$, where $\overline{} = (14)(23)$ is conjugation over $\mathbb{Q}(c)$. Then G_D is generated by that conjuagation and $\sigma = (1234)$.

Conversely, given that D factorises over $\mathbb{Q}(c)$, the cubic resolvent C_D of D must have a rational zero $\alpha_1\alpha_3 + \alpha_2\alpha_4$. The other two zeros $\alpha_1\alpha_2 + \alpha_3\alpha_4$ and $\alpha_1\alpha_4 + \alpha_2\alpha_3$ are invariant under the conjugation but are transposed by σ and, for that matter, also by the 4-cycle $\tau = (1243)$.

If these other zeros of C_D are rational then both σ and τ must be involutions commuting with the conjugation. Then, recalling that D is irreducible over $\mathbb{Q}$, its Galois group G_D is the Viergruppe $\mathcal{V}$. If the pair of zeros is irrational but D factorises over the splitting field of C_D then τ generates G_D and the Galois group of D is the cyclic group $\mathcal{C}_4$. Incidentally, we use the helpful remarks [10, Algorithm 4.2 at page 10], explicitly to distinguish the case $\mathcal{C}_4$ from $\mathcal{D}_4$.

Even calculations. We investigate each case $m = 12, 10, 8, 6, 4$ in detail using the data listed in [18]. For example, the cases $m = 12$ and $m = 10$ are given by

$$\text{(7)}\quad v_{12}(t) = (t-1)(2t-1)(3t^2-3t+1)(2t^2-2t+1)/t^4\,; \qquad w_{12}(t) = -(6t^4-16t^3+14t^2-6t+1)/2t^3\,;$$

$$\text{(8)}\qquad v_{10}(t) = \frac{t^3(2t-1)(t-1)}{(t^2-3t+1)^2}\,; \quad w_{10}(t) = \frac{2t^3-2t^2-2t+1}{2(t^2-3t+1)}\,.$$

Here the parameter t runs through all 'regular' elements of $\mathbb{Q}$; in both cases the irregular rational values are $t = 1$, $t = 1/2$, and $t = 0$.

By Theorem 1(c) we know that $D_m(x;t)$ factorises over $\mathbb{Q}\big(c(t)\big)$. If it also factorises over $\mathbb{Q}$ it must do so as a product $(x^2 - px + q)(x^2 + px + q')$. One solves (rather, Maple [12] solves) this condition for $p = p(t)$, in each case obtaining two polynomial equations in p and t, with one an elliptic curve and the other a quadratic in an auxiliary variable. The condition that its discriminant be a square also is an elliptic curve.

In the case $m = 12$, both of these equations ultimately transform birationally (here PARI-GP [14] lends a hand) to the minimal model $y^2 = x^3 - x^2 + x$. This is is 24A4 in John Cremona's tables [6]; thus with conductor 24. It has rank 0 and cyclic torsion of order 4; the torsion points are $(0,0)$, $(1,1)$, $(1,-1)$, and ∞ and correspond to irregular values of t. So $D_{12}(x;t)$ is irreducible over $\mathbb{Q}$ for all regular $t \in \mathbb{Q}$.

When, instead, we check the cubic resolvent, for example when $m=10$, we find that its rational zero is

$$\left(2\,t^3-4\,t^2+4\,t-1\right)\left(2\,t^3-4\,t^2+1\right)\,/\,2\left(t^2-3\,t+1\right)^2$$

and if the discriminant of the remaining quadratic factor of C_D is a square then the elliptic curve $s^2=(4t^2-2t-1)(2t-1)$ must have admissible rational points. However, its minimal model $y^2=x^3+x^2-x$ is 20A2 in Cremona's tables and it has rank 0 and cyclic torsion of order 6. The torsion points are $(0,0)$, $(\pm1,\pm1)$, and ∞ and correspond to irregular values of t.

Following *both* the alternative approaches for each of $m=12$ and $m=10$ verifies a result we have used above, to wit Tran's result [18, p. 400*ff*] that neither $\kappa_{12}(t)$ nor $\kappa_{10}(t)$ — see § 4.3 at page 72 above — can be the square of a rational for regular $t\in\mathbb{Q}$.

For these and the remaining even cases $m=8$, $m=6$, and $m=4$, where we know that $k=\kappa_m(t)$ may be a square for some regular t, we followed both approaches and found that when $D_m(x;t)$ is irreducible its Galois group G_D is the dihedral group $\mathcal{D}_4$ except in the cases encapsulated in the following table.

m	(v,w)	$G_D=\mathcal{C}_2\times\mathcal{C}_2$	$G_D=\mathcal{C}_4$
4	$(t,\frac12)$	$t=\frac{1}{16}(s^2-1)$	$t=-\frac{1}{16}/(s^2+1)$
6	$(t(t-1),1-t/2)$	$t=8/(9-s^2)$	–
8	$((t-1)(2t-1),$ $-(2t^2-4t+1)/2t)$	–	–
10	$\big(t^3(2t-1)(t-1)/(t^2-3t+1)^2,$ $2t^3-2t^2-2t+1/2(t^2-3t+1)\big)$	–	$*$
12	$\big((t-1)\,(2\,t-1)\,\big(3\,t^2-3\,t+1\big)\,\big(2\,t^2-2\,t+1\big)/t^4,$ $-\,(6t^4-16t^3+14t^2-6t+1)/2t^3\,\big)$	–	–

Table I

Moreover for m even, $D_m(x,t)$ is irreducible except in the following cases:

m	(v,w)	$D=f_1f_2$	$D=f_1f_2f_3$	$D=f_1f_2f_3f_4$
4	$(t,\frac12)$	$t=\begin{cases}-s^2,\\ 4s^4-s^2\end{cases}$	$t=-\left(\frac{s^2-1}{4}\right)^2$	$t=-\left(\frac{s^3-s}{(s^2+1)^2}\right)^2$
6	$(t(t-1),1-t/2)$	$t=\begin{cases}1-s^2\\ \frac{(1+s^2)^2}{3s^2+1}\end{cases}$	$t=1-\left(\frac{s^2-1}{s^2+3}\right)^2$	–
8	$((t-1)(2t-1),$ $-(2t^2-4t+1)/2t)$	$t=1/(s^2+1)$	†	–

Table II

The notes $*$ and $\dagger$ refer to two special cases we resolved not to attempt to resolve. We found that rational points (t,u) on the curve

$$u^2 = (t-1)(4t^2-2x-1)(2t-1)(t^2-3t+1)t$$

give rise to cases $D_{10}(x;t)$ with Galois group $\mathcal{D}_4$; and rational points on the curve

$$u^2 = (t^4-1)(t^2+2t-1)$$

give cases where $D_8(x;t)$ splits into three factors over $\mathbb{Q}$. We expect that neither curve provides regular rational such t.

We leave the degenerate case $m=2$, where $D(x;u,k)=(X^2+u)^2-k$, as an easy exercise. ∎

Odd remarks. In the odd cases $m=9$, $m=7$, and $m=5$, the final remark following Theorem 2 at page 73, together with the detailed continued fraction expansions[‡] in [18], shows that

$$\begin{aligned}\bigl(x-\tfrac12(t^3-3t^2+4t-1)\bigr) &\quad \text{divides } D_9(x;t)\,,\\ \bigl(x+\tfrac12(t^2-3t+1)\bigr) &\quad \text{divides } D_7(x;t)\,,\\ \bigl(x-\tfrac12(t+1)\bigr) &\quad \text{divides } D_5(x;t)\,;\end{aligned}$$

here

$$\begin{aligned} v_9(t)=t^2(t-1)(t^2-t+1),\quad w_9(t)=-\tfrac12(t^3-t^2-1),\qquad t\in\mathbb{Q}\setminus\{0,1\}\,,\\ v_7(t)=t^2(t-1),\quad w_7(t)=-\tfrac12(t^2-t-1),\qquad t\in\mathbb{Q}\setminus\{0,1\}\,,\\ v_5(t)=t,\quad w_5(t)=-\tfrac12(t-1),\qquad t\in\mathbb{Q}\setminus\{0\}\,.\end{aligned}$$

For completeness we remark that in these cases the residual cubic factor $G_m(x;t)$ is reducible in the case $m=5$ and $t=s^2(s+1)/(s+1)$ and that then the surviving quadratic factor is irreducible. With finitely many possible exceptions, namely unlikely rational points on certain curves[§] of genus more than 1, the Galois groups of the irreducible $G_m(x;t)$ is always $\mathcal{S}_3$.

The case $m=3$ is degenerate; however, plainly

$$D_3(x;v,w)=(x^2-w^2)^2+4v(x+w)=(x+w)(x^3-wx^2-w^2x-4v+w^3)=:(x+w)F\,.$$

If F is irreducible, then its Galois group is $\mathcal{A}_3$ if and only if $v=8t^2w^3/(27t^2+1)$. Further, F has a zero r when $v=(w+r)(w-r)^2/4$; specifically

$$F=(x-r)(x^2-(w-r)x-w^2-rw+r^2).$$

F splits as the product of three linear factors when $v=8w^3(s^2-1)^2/\bigl((s^2+3)^3\bigr)$. The reader may find it a useful exercise to extract other details.

[‡] As always, such data must be used modulo typos. Worse, the notation of [18] is slightly different from that of here and in [16]; its v is our $4v$.

[§] The respective discriminants $F_m(t)$ of the cubic factors are $F_7(t)=t(t-1)(t^3-8t^2+5t+1)$, $F_9(t)=t(t-1)(t^2-t+1)(t^3-6t^2+3t+1)$, and $F_5(t)=t(t-1)(t^3-8t^2+5t+1)$. The last case is Cremona's curve 20A2, which has rank 0 and torsion 2. We saw that $G_7(x;t)$ is irreducible because a putative rational zero corresponds to a rational point on the curve 14A4 with rank 0 and torsion 2. We found a complicated genus 2 curve not warranting report whose rational points might allow $G_9(x;t)$ to factorise.

References

[1] William W. Adams and Michael J. Razar, 'Multiples of points on elliptic curves and continued fractions', *Proc. London Math. Soc.* **41** (1980), 481–498.

[2] Roberto M. Avanzi and Umberto M. Zannier, 'Genus one curves defined by separated variable polynomials and a polynomial Pell equation', *Acta Arith.* **99**.3 (2001), 227–256.

[3] T. G. Berry, 'On periodicity of continued fractions in hyperelliptic function fields', *Arch. Math.* **55** (1990), 259–266.

[4] Enrico Bombieri and Paula B. Cohen, 'Siegel's lemma, Padé approximations and Jacobians' (with an appendix by Umberto Zannier, and dedicated to Enzio De Giorgi), *Ann. Scuola Norm. Sup. Pisa* Cl. Sci. (4) **25** (1997), 155–178.

[5] D.G. Cantor, 'Computing in the Jacobian of a hyperelliptic curve', *Math. Comp.* **48**.177 (1987), 95–101.

[6] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge University Press, 1997. Available on-line at http://www.maths.nott.ac.uk/personal/jec/book/amec.html.

[7] Christian Friesen, 'Continued fraction characterization and generic ideals' in [8], 465–474.

[8] David Goss, David R. Hayes and Michael I. Rosen eds., *The arithmetic of function fields*, Proceedings of the workshop held at The Ohio State University, Columbus, Ohio, June 17–26, 1991. Ohio State University Mathematical Research Institute Publications, **2**. Walter de Gruyter & Co., Berlin, 1992. viii+482 pp.

[9] Isabelle Hardy and Yves Hellegouarch, 'Fractions continues normales dans un corps de fonctions hyperelliptiques', *Acta Arith.* **101**.1 (2002), 19–37.

[10] Alexander D. Healy, 'Resultants, resolvents, and computation of Galois groups', at http://www.alexhealy.net/papers/math250a.pdf.

[11] Kristin E. Lauter, 'The equivalence of the geometric and algebraic group laws for Jacobians of genus 2 curves', to appear in Proceedings of the conferences in memory of Ruth Michler, AMS *Contemporary Mathematics* Series.

[12] Maple. See http://www.maplesoft.com/.

[13] B. Mazur, 'Modular curves and the Eisenstein ideal', *Inst. Hautes Études Sci. Publ. Math.* **47** (1977), 33–186.

[14] PARI-GP. See http://pari.math.u-bordeaux.fr.

[15] Alfred J. van der Poorten, 'Non-periodic continued fractions in hyperelliptic function fields', (Dedicated to George Szekeres on his 90th birthday), *Bull. Austral. Math. Soc.* **64** (2001), 331–343.

[16] ———, 'Periodic continued fractions and elliptic curves', to appear in *High Primes and Misdemeanours*: lectures in honour of the 60th birthday of Hugh Cowie Williams, Alf van der Poorten and Andreas Stein eds., Fields Institute Communications Series, American Mathematical Society, 2004, 13pp.

[17] Alfred J. van der Poorten and Xuan Chuong Tran, 'Quasi-elliptic integrals and periodic continued fractions', *Monatshefte Math.*, 131 (2000), 155-169.

[18] ———, 'Periodic continued fractions in elliptic function fields', in Claus Fieker and David R. Kohel eds, *Algorithmic Number Theory* (Proc. Fifth International Symposium, ANTS-V, Sydney, NSW, Australia July 2002), Springer Lecture Notes in Computer Science 2369 (2002), 390–404.

[19] Wolfgang M. Schmidt, 'On continued fractions and diophantine approximation in power series fields', *Acta Arith.* **95** (2000), 139–166.

[20] Ethan Street, 'Pell's equation and Laurent fields', manuscript, 2003.

Dipartimento di Matematica, Università degli Studi Roma Tre
L.go San Leonardo Murialdo, 1 c.a.p. I-00146 Roma, Italy
E-mail address: pappa@mat.uniroma3.it (Francesco Pappalardi)

Centre for Number Theory Research
1 Bimbil Place, Killara, Sydney NSW 2071, Australia
E-mail address: alf@math.mq.edu.au (Alf van der Poorten)